

## Disaster Recovery

### Cisco ASA configuration

#### Static IP Addresses

```
75.144.109. *hidden* E1 Port IVM-PIX
75.144.109. *hidden* Points to 192.*hidden*.6 Points to 192.168. *hidden*
75.144.109.1*hidden* S*hidden*.g.com Points to 192.168. *hidden*
75.144.109.1*hidden* iv*hidden*.com Points to 192.168. *hidden*
75.144.109.1*hidden* sup*hidden*.ing.net Points to 192.168. *hidden*
75.144.109.1*hidden* mail.in*hidden*.g.com Points to 192.168. *hidden*
75.144.109.1*hidden*
75.144.109.1*hidden*
75.144.109.1*hidden*
```

```
75.144.109.1*hidden* Cisco PIX 515e( Seen by outside) iv*hidden*ltime.net
inter*hidden*.ng.com
iv*hidden*ime.com
75.144.109. *hidden* E1 Port IVM-PIX
```

Router password: \*hidden\*

Router VPN password: \*hidden\*

### Change ASA IP address [ DMZ internal address ]

```
CONFIG T
INT VLAN1
IP ADDRESS 192.168.0.254 255.255.255.0
SH INT VLAN1
PING 192.168.0.254
```

### Change ASA IP address [ OUTSIDE (Comcast) address ]

```
CONF IG T
INT VLAN3
IP ADDRESS 75.144.109.98 255.255.255.0
SH INT VLAN3
PING 75.144.109.98
```

### Shutdown interface?

If the interfaces are seen as "administratively down", try reissuing the interface config command.

```
CONF T
```

INT E0

## **One-to-One NAT Configuration**

PIX configured to handle traffic to 97.158.253.26 (example only). Allow all incoming traffic to be forwarded to web server which has an IP address of 192.168.1.100. Only WWW and DNS (Port 53) traffic is allowed to access it via an access control list applied to the outside interface.

```
ACCESS-LIST INBOUND PERMIT ICMP ANY ANY
ACCESS-LIST INBOUND PERMIT TCP ANY HOST 97.158.253.26 EQ WWW
ACCESS-LIST INBOUND PERMIT TCP ANY HOST 97.158.253.26 EQ 53
ACCESS-LIST INBOUND PERMIT UDP ANY HOST 97.158.253.26 EQ 53
```

```
ACCESS-GROUP INBOUND IN INTERFACE OUTSIDE
```

```
STATIC (INSIDE,OUTSIDE) 97.158.253.26 192.168.1.100 NETMASK
255.255.255.255 0 0
```

Outbound NAT Configuration (Many-to-One NAT)

Here we allow connections originating from servers connected to the inside (private/protected) interface with an IP address in the range 192.168.1.0 to 192.168.1.255 to be NAT-ted to the IP address of the outside (Public/unprotected) interface of the firewall which is 97.158.253.25 :

```
GLOBAL (OUTSIDE) 1 INTERFACE
NAT (INSIDE) 1 192.168.1.0 255.255.255.0 0 0
```

## **Static IP Addresses**

In this example, the ISP has assigned the Internet subnet 97.158.253.24 with a mask of 255.255.255.248 (/29). The IP address selected for the PIX is 97.158.253.25, the default gateway is 97.158.253.30

```
IP ADDRESS OUTSIDE 97.158.253.25 255.255.255.248
IP ADDRESS INSIDE 192.168.1.1 255.255.255.0
ROUTE OUTSIDE 0.0.0.0 0.0.0.0 97.158.253.30
```

In this example, the IP address of the PIX is 192.168.1.1. As the PIX will be acting as your default gateway to the internet, you will have to set the default gateway on all your servers to be 192.168.1.1

**Note:** When you receive your own /29 allocation all the IPs are exclusively yours whether you use them or not. This can be viewed as being wasteful in the eyes of some ISPs. Some service providers now use PPPoE with DHCP IP address reservations based on your MAC address. It appears to be an attempt to conserve

on IP addresses by placing many customers on a large shared network that allows the ISP to add and subtract allocated IPs at will. This means that the ISP, and not its customers, are in possession of all unused IP addresses.

**NFRAME Configuration**  
**( Configure interfaces )**

CONF T

INT E

End of sample fragment